Docket No. 1293.1191/MDS/JGM

#4

JC986 U.S. PTO 09/833793 04/13/01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	
	)	
Jung-wan KO, et al.	)	
	)	Group Art Unit: To be assigned
Serial No.: NEW	)	
	)	Examiner: To be assigned
Filed: April 13, 2001	)	

For: HIGH SPEED COPY PROTECTION METHOD

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Korean Patent Application No. 2000-31028, filed June 7, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By: _____
Michael D. Stein
Registration No. 37,240

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

Date: 4/13/01

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

#4

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 31028 호
Application Number

출 원 년 월 일 : 2000년 06월 07일
Date of Application

출 원 인 : 삼성전자 주식회사
Applicant(s)

CERTIFIED COPY OF PRIORITY DOCUMENT

2000 년 07 월 05 일

특 허 청
COMMISSIONER

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 0007
【제출일자】 2000.06.07
【국제특허분류】 G11B
【발명의 명칭】 고속 복제 방지 방법
【발명의 영문명칭】 High speed copy protection method
【출원인】
【명칭】 삼성전자 주식회사
【출원인코드】 1-1998-104271-3
【대리인】
【성명】 이영필
【대리인코드】 9-1998-000334-6
【포괄위임등록번호】 1999-009556-9
【대리인】
【성명】 조혁근
【대리인코드】 9-1998-000544-0
【포괄위임등록번호】 2000-002820-3
【대리인】
【성명】 이해영
【대리인코드】 9-1999-000227-4
【포괄위임등록번호】 2000-002816-9
【발명자】
【성명의 국문표기】 고정완
【성명의 영문표기】 KO,Jung Wan
【주민등록번호】 600925-1119917
【우편번호】 449-830
【주소】 경기도 용인시 이동면 서리 684-6
【국적】 KR
【발명자】
【성명의 국문표기】 김병준
【성명의 영문표기】 KIM,Byung Jun
【주민등록번호】 681223-1671318

【우편번호】 442-192

【주소】 경기도 수원시 팔달구 우만2동 29번지 주공아파트 207동 404호

【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이영필 (인) 대리인 조혁근 (인) 대리인 이해영 (인)

【수수료】

【기본출원료】	18	면	29,000 원
【가산출원료】	0	면	0 원
【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원

【합계】 29,000 원

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명에는 고속 복제 방지 방법이 개시되어 있다. 본 발명은 제2 암호화 키 데이터가 포함된 원문의 일부 영역은 제1 암호화 키를 이용하여 암호화하고, 제2 암호화 키를 이용하여 원문의 나머지 영역을 암호화하여 암호문을 전송하는 단계를 포함하여, 고속 처리가 필요한 대량의 암호문 데이터는 공통키 방식의 키를 이용해서 처리하고, 암호문 데이터 중의 일부는 크기가 큰 키의 공통키를 사용하거나 공개키 방식의 키를 사용해서 처리해서 속도와 안전성을 동시에 만족시킬 수 있다.

【대표도】

도 4

【명세서】

【발명의 명칭】

고속 복제 방지 방법{High speed copy protection method}

【도면의 간단한 설명】

도 1은 일반적인 암호화 장치의 블록도이다.

도 2는 종래의 복제 방지 방법의 흐름도이다.

도 3은 본 발명에 의한 고속 복제 방지 방법을 설명하기 위한 개략도이다.

도 4는 본 발명에 의한 고속 복제 방지 방법의 일 실시예에 따른 흐름도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<5> 본 발명은 디지털 데이터 암호화 분야에 관한 것으로, 특히 이중 암호화 키를 이용한 고속 복제 방지 방법에 관한 것이다.

<6> 디지털 저장 매체, 인터넷, 전자 상거래 등이 확산됨에 따라 보다 많은 분야에서 다양한 목적으로 암호화 방법이 사용되고 있다. 암호화 방법이 사용되는 대표적인 것으로는 보안, 이용자 신원 확인(authentication) 그리고 복제 방지 등이 있다. 이러한 암호화 방법에서 현재 가장 널리 사용되는 것이 40 비트 또는 56 비트 크기의 키를 이용한 공통키(common key) 암호화 방법과 512 비트 또는 1024 비트 크기 등의 키를 이용한 공개키(public key) 암호화 방법이다. 하지만 암호화에 사용되는 키의 크기가 커지게 되면 안전성은 높아지나 이를 위한 계산량이 급증하고, 처리 속도가 현저하게 느려지게 된다

<7> 도 1은 일반적인 암호화 장치의 블록도로서, 원문을 암호화해서 암호문을 제공하는 송신자(sender: 100)와 송신자(100)로부터 암호화에 사용된 키를 전송받아서 암호문을 복호화해서 원문을 복원하는 수신자(receiver: 200)로 이루어진다. 보다 진보된 경우에는 송신자(100)와 수신자(200) 이외에 키의 공개, 갱신 또는 배포 등을 담당하는 제3 자가 개입할 수도 있으나 여기에선 생략한다.

<8> 송신자(100)는 암호화 키를 이용해서 원문을 암호화해주는 암호화기(encryptor: 110) 그리고 암호화 키를 전송하기 위해서 안전한 전송 통로(10)를 확보하기 위한 인증기(authenticator: 120) 등을 가진다. 수신자(200)는 암호화에 사용된 키를 전송받기 위해 필요한 안전한 전송 통로(10)의 확보를 위한 인증기(210)와 전송받은 암호화 키를 이용해서 암호문을 복호화하는 복호화기(decryptor: 220) 등을 가진다.

<9> 도 2는 종래의 복제 방지 방법의 흐름도로서, 송신자 또는 수신자가 상대편 수신자 또는 송신자에게 송신 또는 수신을 의뢰를 할 수 있는 데, 즉, 송신자가 송신을 위해 수신자에게 의뢰를 하면(S1 단계) 수신자의 응답을 통해 수신자가 준비되어 있는 지를 체크한다(S2 단계). 마찬가지로 수신자가 수신을 위해 송신자에게 의뢰를 하면(S3 단계) 송신자의 응답을 통해 송신자가 준비되어 있는 지를 체크한다(S4 단계).

<10> 상기 S2 단계에서 수신자가 수신할 준비가 되어 있거나 상기 S4 단계에서 송

신자가 송신할 준비가 되어 있으면 송신자가 수신자를 인증한다(S5 단계). 이때, S5 단계에서 송신자가 수신자에게 인증용 챌린지(challenge)를 전송해서 수신자가 이 인증용 챌린지에 대한 응답을 송신자에게 전송하면 송신자는 전송된 응답을 비교를 통해 인증이 제대로 되었는 지를 판단한다(S6 단계). S6 단계에서 판단 결과가 인증이 제대로 되었으면 다시 수신자가 송신자를 인증하고(S7 단계), 그렇지 않으면 인증을 중단한다(S8 단계). 상기 S7 단계에서는 수신자가 송신자에게 인증용 챌린지를 전송해서 송신자가 이 인증용 챌린지에 대한 응답을 수신자에게 전송하면 수신자는 전송된 응답을 비교를 통해 인증이 제대로 되어 있는 지를 판단한다(S9 단계). S9 단계에서 인증이 제대로 되었으면 인증키를 생성하고 안전한 전송 통로를 확보하게 되고(S10 단계), 그렇지 않으면 인증을 중단한다(S11 단계). S1 단계 내지 S11 단계는 인증 단계라고 지칭할 수 있다.

<11> S10 단계에서 안전한 전송 통로가 확보되면 암호화 키로 원문을 암호화해서 암호문을 전송한다(S12 단계). 암호화에 사용된 키를 상기 S10 단계에서 생성된 인증키를 이용하여 암호화해서 안전한 전송 통로로 전송하고(S13 단계), 안전한 전송 통로를 통해 수신된 암호화 키로 암호문을 복호화해서 원문을 복원한다(S14 단계).

<12> 도 2에서 설명된 암호문의 암호화 방법은 공통키 암호화 방법이므로, 암호화와 복호화시 동일한 암호화 키가 사용된다. 전송 통로는 키를 전송하기 위해 필요한 어느 정도 안전이 보장된 전송 통로와 암호화된 데이터를 전송하는 일반 통로로 구성된다. 암호화 키가 없이는 복호화가 불가능하다는 전제하에 암호문은 일반 통로를 이용하게 되며, 이 일반 통로는 인터넷 망 또는 전화망 등과 같은 개방 통로(public path)로 지칭될 수 있다.

<13> 암호화에 사용된 키를 안전하게 전송하기 위한 가장 일반적인 전송 방법은 인증을

통해 확보된 안전한 전송 통로로 소정의 암호화 방법을 사용하여 전송하는 것이다. 즉, 인증을 통해 확보된 안전한 전송 통로로 암호화된 키를 전송하는 도 2에 도시된 S13 단계에서는 문서의 암호화에 사용된 것과는 다른 암호화 방법을 사용하며, 암호화 키 보다 큰 크기의 인증키를 사용한 암호화 방법이 주로 사용되며, 이때, 인증키의 크기가 커짐에 따라 안전성은 증가하는 반면 처리 속도는 저하된다.

<14> 송신자는 안전한 전송 통로를 통해 수신자에게 암호화 키를 전송하고(도 2의 S13 단계), 전송할 원문 데이터는 이 암호화 키를 이용해서 공통키 암호화 방법으로 암호화한다(도 2의 S12 단계). 이때, 사용되는 공통키 암호화 방법은 주로 40비트 또는 56 비트 크기의 암호화 키를 이용하므로, 안전성은 저하되지만 처리 속도가 증가하여 대량의 데이터 처리에 용이하다. 암호화된 암호문은 안전하지 않은 통로를 통해서 또는 공개된 장소를 통해서도 수신자에게 전송될 수 있다. 수신자는 인증을 거친 안전한 전송 통로로 전송된 암호화 키를 전송받은 후에 복호화하여 암호화 키를 구하고, 이를 이용해서 공통키 암호화 방법으로 처리된 암호문을 복호화하여 원문을 복원한다.

<15> 여기서, 암호화와 복호화시 동일한 키를 사용하므로 이를 공통키(또는 대칭키) 암호화 방법이라고 하며, 암호화와 복호화에 각기 다른 키를 사용하는 경우에는 공개키(또는 비대칭키) 암호화 방법이라고 한다. 대개 공통키 암호화 방법은 키의 크기가 작고 암호화 방법이 단순해서 안전성은 상대적으로 떨어지지만 처리 속도가 빠르며, 공개키 암호화 방법은 키의 크기가 대체로 커서 처리 속도는 느리지만 안전성은 상당히 높다. 그래서 주로 안전한 전송 통로를 확보하기 위한 인증 단계에서 공개키를 사용하고, 원문을 암호화하는 데이터 처리 단계에서는 공통키를 사용한다.

<16> 한편, 고성능의 컴퓨터가 개인에게 보급되고 성능 또한 계속 향상되면서 이러한 암

호화 방법은 안전성 측면에서 상당히 위협을 받게 되었다. 즉, 계산 능력이 향상된 개인용 컴퓨터는 일반적인 공간에 공개된 암호문에 대해서 암호화 키가 없이도 공격할 수 있는 충분한 능력을 갖추게 된 것이다. 암호화 키의 크기가 작으므로 단순한 반복적인 작업을 수행해서 암호화에 사용된 키를 찾아낼 수가 있게 되고, 이를 이용해서 복호화가 가능하게 된다.

<17> 현재 주로 사용되고 있는 40 비트 또는 56 비트 크기의 공통키 암호화 방법은 조만간 효력이 없어질 수 있으며, 컴퓨터를 제외한 연산 능력이 떨어지는 정보 가전 기기에서 128 비트 이상의 암호화 방법의 사용은 안전성은 높일 수 있지만 연산 능력의 제한으로 처리 속도를 저하시키게 된다. 더군다나 512 비트 이상의 공개키 방식의 도입은 더욱 더 어려운 실정이다. 그러나, 앞으로는 컴퓨터가 아닌 정보 가전 기기에서도 상거래와 같은 높은 수준의 안전성이 확보되어야 하므로 현재의 암호화 방법은 안전성과 속도 양쪽 모두에도 만족시킬 수 없는 문제점이 있었다.

【발명이 이루고자 하는 기술적 과제】

<18> 상기한 문제점을 해결하기 위하여, 본 발명의 목적은 이중 키 암호화 방법을 이용한 고속 복제 방지 방법을 제공하는 데 있다.

<19> 본 발명의 다른 목적은 안전성을 높이기 위해 제1 암호화 키를 사용해서 원문의 일부를 암호화하고 고속 처리를 위해서 제2 암호화 키를 사용하여 원문의 나머지를 암호화하는 고속 복제 방지 방법을 제공하는 데 있다.

<20> 상기한 목적들을 달성하기 위하여, 본 발명에 의한 고속 복제 방지 방법은 송신자와 수신자와의 디지털 데이터 전송시 디지털 데이터의 복제를 방지하는 방법에 있어서:

제2 암호화 키 데이터가 포함된 원문의 일부 영역은 제1 암호화 키를 이용하여 암호화하고, 제2 암호화 키를 이용하여 원문의 나머지 영역을 암호화하여 암호문을 전송하는 단계를 포함함을 특징으로 하고 있다.

<21> 본 발명에 의한 고속 복제 방지 방법은 제1 암호화 키, 원문을 일부 영역과 나머지 영역으로 분할하는 영역 분할 정보와 제2 암호화 키와 관련된 정보를 안전한 전송 통로를 이용하여 전송하는 단계를 더 포함함을 특징으로 하고 있다.

<22> 또한, 본 발명에 의한 고속 복제 방지 방법은 안전한 전송 통로를 통해 전송된 제1 암호화 키와 영역 분할 정보를 이용하여 암호문 일부 영역을 복호화하는 단계, 수신된 제2 암호화 키와 관련된 정보를 이용하여 복호화된 일부 영역에서 제2 암호화 키를 추출하는 단계 및 추출된 제2 암호화 키를 이용하여 암호문의 나머지 영역을 복호화하여 원문을 복원하는 단계를 더 포함함을 특징으로 하고 있다.

【발명의 구성 및 작용】

<23> 이하, 첨부된 도면을 참조하여 본 발명에 의한 고속 복제 방지 방법의 바람직한 실시예를 설명하기로 한다.

<24> 도 3은 본 발명에 의한 고속 복제 방지 방법을 설명하기 위한 개략도로서, 송신자는 암호화할 원문 데이터의 특정 위치에 있는 데이터를 제2 암호화 키로서 추출한다. 이 제2 암호화 키 데이터의 위치는 가변될 수 있으며, 고정되어 사용될 수도 있다. 제2 암호화 키의 크기는 기존에 사용하던 공통키 암호화 방법에서 사용하던 것과 같을 수도 있고, 다른 크기로 사용될 수도 있다.

<25> 한편, 제1 암호화 키는, 공통키 암호화 방법을 사용한다면, 기존의 것보다 큰 크기

의 제1 암호화 키를 사용한다. 공개키 암호화 방법을 사용한다면, 제1 암호화 키는 기존의 공개키 방식에서 사용되던 것과 동일한 크기라도 상관없다.

<26> 제1 암호화 키를 이용해서 원문 데이터의 일정 영역을 암호화한다. 이때, 일정 영역은 반드시 제2 암호화 키로 추출되어 사용될 데이터가 포함되도록 영역(이하 제1 영역(A)라고 함)을 설정해야 한다. 원문의 나머지 영역을 제2 영역이라고 지칭한다. 이 제1 영역과 제2 영역의 크기는 가변될 수 있지만, 송신자와 수신자의 상호간에 각 암호화 키들(제1 및 제2 암호화 키)의 크기와 분할 영역은 동일해야 한다.

<27> 즉, 제1 영역(A)과 제2 영역(B)을 미리 정하고, 제1 영역(A)에서 제2 암호화 키를 추출한 후에 제1 영역(A)을 제1 암호화 키로 암호화하고, 제2 영역(B)을 제2 암호화 키를 이용해서 암호화한다. 안전한 전송 통로를 확보한 이후 제1 암호화 키를 안전한 전송 통로를 통해 수신자에게 전송하고, 암호문을 전송한다. 여기서, 암호문은 안전성이 확보되지 않은 일반적인 통로로 전송될 수 있다. 상술한 방법으로 다음 원문 데이터를 암호화할 수 있으며, 이때 사용하는 제1 암호화 키는 같지만, 제1 영역에서 추출된 제2 암호화 키는 다른 값이 될 수 있다.

<28> 수신자는 안전한 전송 통로를 통해 전송받은 제1 암호화 키를 이용해서 제1 영역(A)을 복호화하고, 복호화된 제1 영역(A)에서 제2 암호화 키를 추출해서 제2 영역(B)을 복호화하면 원문을 제공할 수 있다.

<29> 또한, 인증 단계를 거쳐 안전한 전송 통로를 확보하게 되는 데, 이때 각 영역 분할에 대한 정보(제2 영역의 시작 주소나 제1 영역의 크기 등과 같은 정보)와 함께 수신자의 연산 능력에 맞춰 사용되는 제1 및 제2 암호화 키의 크기 및 제2 암호화 키의 위치, 각 영역의 암호화 방법에 대한 정보를 공유할 수 있게 함으로써, 보다 가변적이고도 안

전한 암호화를 달성할 수 있다.

<30> 따라서, 본 발명에 의한 고속 복제 방지 방법이 도 1에 도시된 일반적인 암호화 장치에 적용될 수 있지만 안전한 전송 통로(10)를 통해 종래에는 원문의 암호화를 위한 암호화 키만을 전송했지만 본 발명에서는 원문의 제1 영역의 암호화를 위한 제1 암호화 키 뿐만 아니라 제2 영역의 암호화를 위한 제2 암호화 키 정보(크기, 위치)와 영역 분할 정보도 안전한 전송 통로(10)를 통해 전송된다. 여기서, 제2 암호화 키를 포함하는 제1 영역은 제2 영역보다 작으며, 제1 암호화 키의 크기는 제2 암호화 키보다 크다.

<31> 본 발명의 일 실시예에 따른 고속 복제 방지 방법의 흐름도인 도 4에 있어서, S101 단계의 인증 단계는 도 2에 도시된 S1 단계 내지 S11 단계에 도시된 동일한 과정을 거쳐 안전한 전송 통로를 확보하게 된다.

<32> 인증 단계(S1 단계)를 거친 후 원문의 일부 영역에서 제2 암호화 키를 추출한다(S102 단계). 제1 암호화 키를 이용하여 원문 중 일부 영역을 암호화한다(S103 단계). 제2 암호화 키를 이용하여 나머지 영역을 암호화해서 암호문을 전송한다(S104 단계). 제1 암호화 키를 안전한 전송 통로로 전송한다(S105 단계). 영역 분할 정보와 제2 암호화 키 정보(크기, 위치)를 안전한 전송 통로로 전송한다(S106 단계).

<33> 한편, 수신자측에서는 수신된 제1 암호화 키와 영역 분할 정보를 이용하여 암호문의 일부 영역을 복호화한다(S107 단계). 역시 수신된 제2 암호화 키의 정보(크기, 위치 등)를 이용해서 복호화된 일부 영역에서 제2 암호화 키를 추출한다(S108 단계). 추출된 제2 암호화 키로 나머지 영역을 복호화한다(S109 단계).

<34> 따라서, 본 발명은 제2 암호화 키를 포함하는 원문 데이터의 일부 영역에는 공통키

암호화 방법을 사용하는 기존보다 크기가 큰 제1 암호화 키를 사용하거나 공개키 암호화 방법을 사용한 제1 암호화 키를 사용해서 안전성을 강화하고, 나머지 원문 데이터는 공통키 암호화 방법을 사용하는 크기가 제1 암호화 키보다는 상대적으로 작은 제2 암호화 키를 사용해서 암호화한다. 이렇게 하면 고속 처리가 필요한 대량의 데이터는 공통키 방식의 키를 사용해서 처리하고, 암호문 데이터 중의 일부는 크기가 큰 키의 공통키를 사용하거나 공개키 방식의 키를 사용해서 처리해서 속도와 안전성을 동시에 만족시킬 수 있다.

<35> 따라서, 본 발명은 기존의 방법에 비해 큰 제1 암호화 키를 사용하면서도 데이터의 대부분인 제2 영역은 여전히 작은 크기의 제2 암호화 키를 이용해서 복호화하므로, 안전성은 증가하면서도 필요한 연산 능력과 처리 시간은 그다지 늘어나지 않는다.

【발명의 효과】

<36> 상술한 바와 같이, 본 발명은 이중의 암호화 키를 사용하여 안전성과 속도 증가를 동시에 개선하는 효과가 있다. 본 발명은 복제 방지의 목적으로 사용되는 다른 암호화 방법과 비교해서 전송되는 키를 일부만 전송하므로, 안전성이 보다 높아지는 효과를 얻을 수 있다. 또한, 본 발명은 원 데이터의 일부를 제2 암호화 키로 사용하므로 안전한 전송 통로로 전송해야 하는 암호화 키는 제1 암호화 키 하나이면 충분하며, 자동적으로 이중 키의 하나인 제2 암호화 키는 항상 가변되는 효과를 가진다. 이로 인해서 각 전송 단위마다 다른 암호화 키를 전송하는 효과를 가지므로 안전성이 보다 강화되는 효과가 있다.

【특허청구범위】

【청구항 1】

송신자와 수신자와의 디지털 데이터 전송시 상기 디지털 데이터의 복제를 방지하는 방법에 있어서:

(a) 제2 암호화 키 데이터가 포함된 원문의 일부 영역은 제1 암호화 키를 이용하여 암호화하고, 상기 제2 암호화 키를 이용하여 원문의 나머지 영역을 암호화하여 암호문을 전송하는 단계를 포함하는 복제 방지 방법.

【청구항 2】

제1항에 있어서, 상기 방법은

(b) 상기 제1 암호화 키, 상기 원문을 일부 영역과 나머지 영역으로 분할하는 영역 분할 정보와 상기 제2 암호화 키와 관련된 정보를 안전한 전송 통로를 이용하여 전송하는 단계를 더 포함하는 복제 방지 방법.

【청구항 3】

제1항에 있어서, 상기 (a) 단계에서는 상기 원문의 일부 영역은 공통키 암호화 방법을 사용한 크기가 큰 제1 암호화 키를 사용하여 암호화하는 것을 특징으로 하는 복제 방지 방법.

【청구항 4】

제1항에 있어서, 상기 (a) 단계에서는 상기 원문의 일부 영역은 공개키 암호화 방법을 사용한 제1 암호화 키를 사용하여 암호화하는 것을 특징으로 하는 복제 방지 방법.

【청구항 5】

제1항에 있어서, 상기 (a) 단계에서는 상기 원문의 나머지 영역은 상기 제1 암호화 키보다 상대적으로 크기가 작은 공통키 암호화 방법을 사용한 제2 암호화 키를 사용하여 암호화하는 것을 특징으로 하는 복제 방지 방법.

【청구항 6】

제1항에 있어서, 상기 제1 암호화 키는 고정되나 제2 암호화 키는 전송 단위마다 가변되는 것을 특징으로 하는 복제 방지 방법.

【청구항 7】

제2항에 있어서, 상기 제2 암호화 키와 관련된 정보는 제2 암호화 키의 크기와 위치 정보등을 포함하는 것을 특징으로 하는 복제 방지 방법.

【청구항 8】

제7항에 있어서, 상기 제2 암호화 키의 위치와 크기는 고정되어 있는 것을 특징으로 하는 복제 방지 방법.

【청구항 9】

제7항에 있어서, 상기 제2 암호화 키의 위치와 크기는 가변되는 것을 특징으로 하는 복제 방지 방법.

【청구항 10】

제2항에 있어서, 상기 원문의 일부 영역은 나머지 영역보다 작게 설정되는 것을 특징으로 하는 복제 방지 방법.

【청구항 11】

제2항에 있어서, 상기 영역 분할 정보는 상기 나머지 영역의 시작 주소 또는 상기 일부 영역의 크기 정보로 구성되는 것을 특징으로 하는 복제 방지 방법.

【청구항 12】

제2항에 있어서, 상기 방법은

(c) 상기 안전한 전송 통로를 통해 전송된 상기 제1 암호화 키와 영역 분할 정보를 이용하여 상기 암호문 일부 영역을 복호화하는 단계;

(d) 상기 안전한 전송 통로를 통해 전송된 제2 암호화 키와 관련된 정보를 이용하여 상기 (c) 단계에서 복호화된 일부 영역에서 제2 암호화 키를 추출하는 단계; 및

(e) 상기 추출된 제2 암호화 키를 이용하여 상기 암호문의 나머지 영역을 복호화하여 원문을 복원하는 단계를 더 포함하는 복제 방지 방법.

【청구항 13】

송신자측에서 제2 암호화 키 데이터가 포함된 원문의 일부 영역을 제1 암호화 키를 이용하여 암호화하고, 원문의 나머지 영역은 상기 제2 암호화 키를 이용하여 암호화한 암호문과 상기 제1 암호화 키, 영역 분할 정보와 제2 암호화 키 정보를 수신자에게 전송할 때 상기 암호문의 복제를 방지하는 방법에 있어서:

(a) 전송되는 상기 제1 암호화 키와 영역 분할 정보를 이용하여 상기 암호문 일부 영역을 복호화하는 단계;

(b) 전송되는 상기 제2 암호화 키 정보를 이용하여 상기 (a) 단계에서 복호화된 일부 영역에서 제2 암호화 키를 추출하는 단계; 및

(c) 상기 추출된 제2 암호화 키를 이용하여 암호문의 나머지 영역을 복호화하여 원문을 복원하는 단계를 포함하는 복제 방지 방법.

【청구항 14】

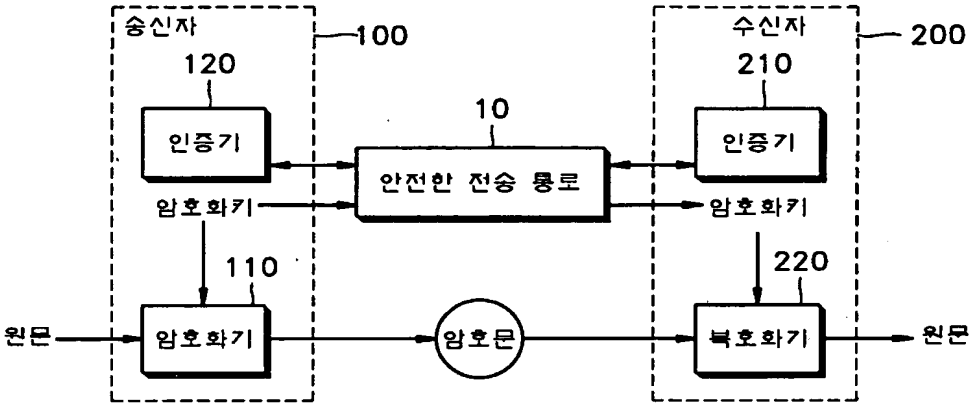
제13항에 있어서, 상기 제1 암호화 키의 크기는 고정되나 제2 암호화 키의 크기는 전송 단위마다 가변되는 것을 특징으로 하는 복제 방지 방법.

【청구항 15】

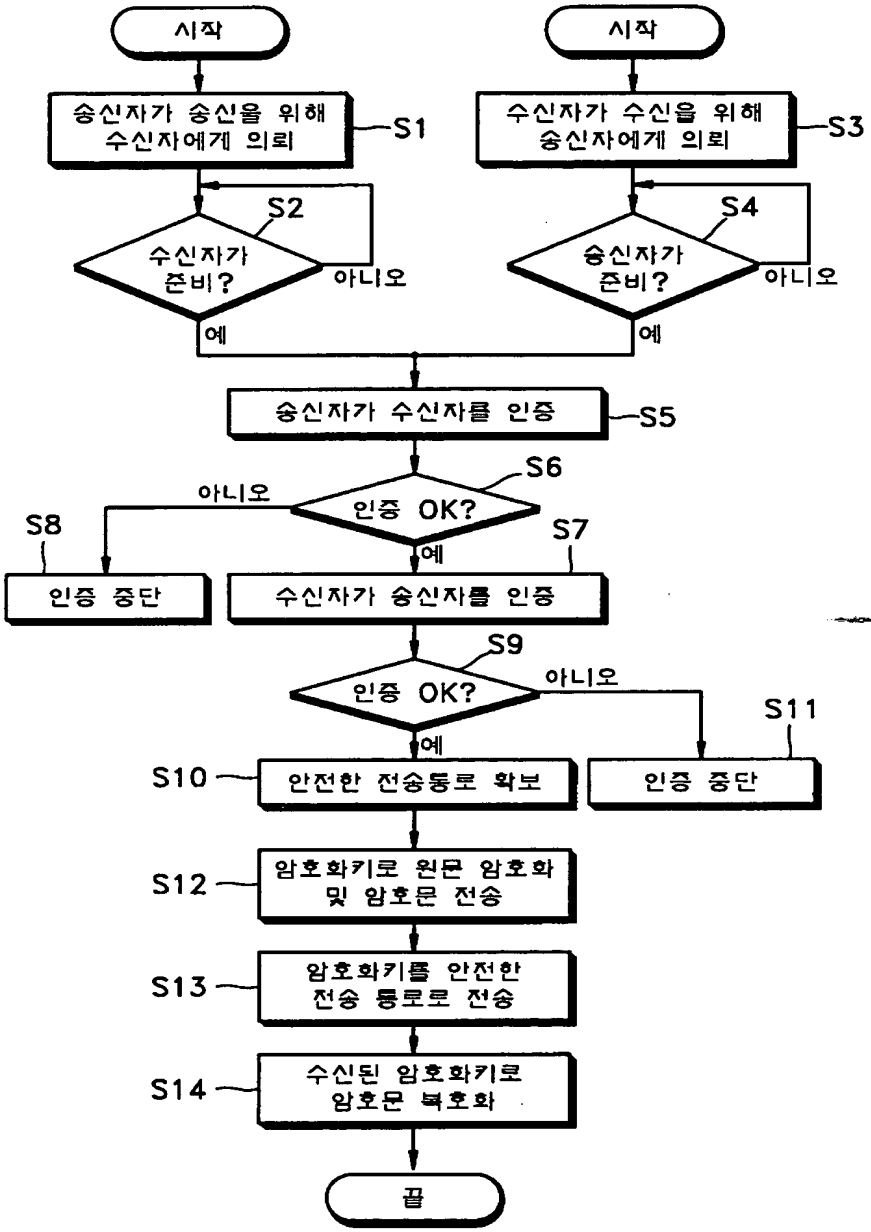
제13항에 있어서, 상기 원문의 일부 영역은 상기 나머지 영역 보다 작게 설정되며, 상기 제1 암호화 키의 크기는 제2 암호화 키보다 크게 설정되는 것을 특징으로 하는 복제 방지 방법.

【도면】

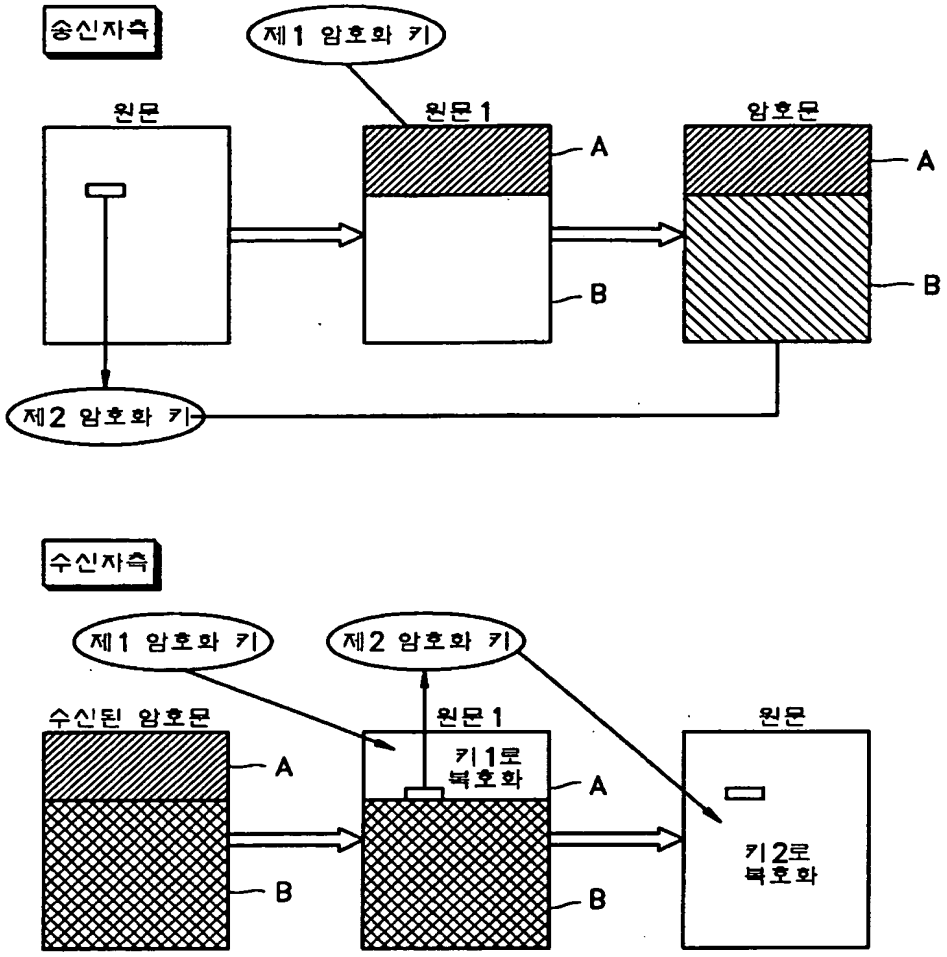
【도 1】


송신자
100
120
인증기
암호화키
110
암호화기
원문
10
안전한 전송 통로
암호문
수신자
200
210
인증기
암호화키
220
복호화기
원문

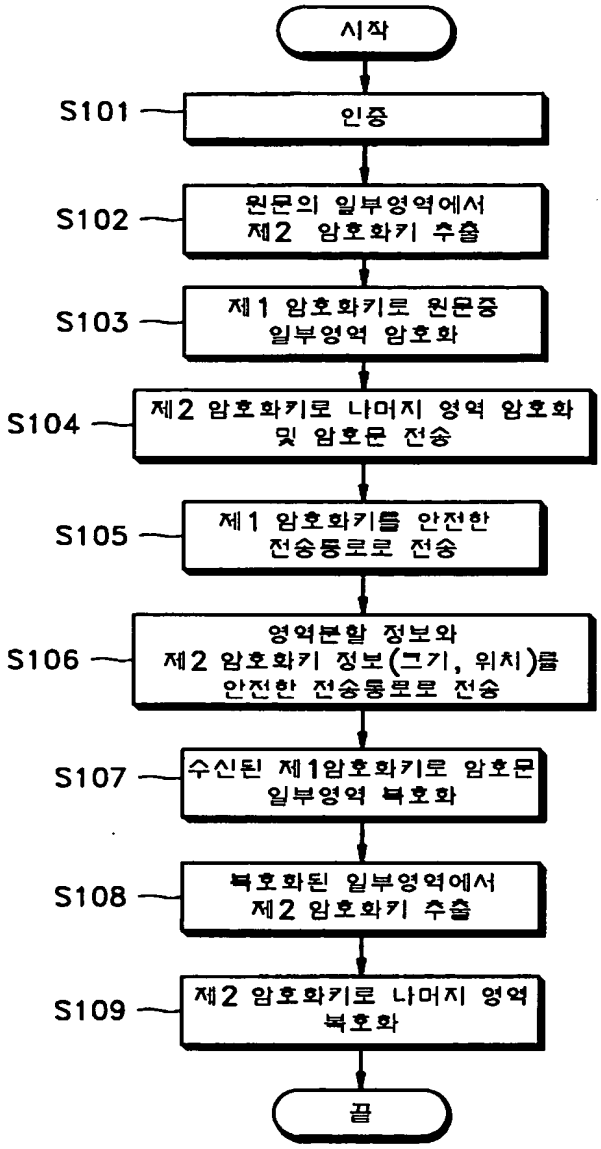
【도 2】


시작
송신자가 송신을 위해 수신자에게 의뢰
S1
수신자가 준비?
S2
아니오
예
시작
수신자가 수신을 위해 송신자에게 의뢰
S3
송신자가 준비?
S4
아니오
예
송신자가 수신자를 인증
S5
인증 OK?
S6
아니오
예
S8
인증 중단
S7
수신자가 송신자를 인증
인증 OK?
S9
아니오
예
S11
인증 중단
S10
안전한 전송통로 확보
S12
암호화키로 원문 암호화 및 암호문 전송
S13
암호화키를 안전한 전송 통로로 전송
S14
수신된 암호화키로 암호문 복호화
끝

【도 3】


송신자측
제1 암호화 키
원문
원문1
암호문
A
B
A
B
제2 암호화 키
수신자측
제1 암호화 키
제2 암호화 키
수신된 암호문
원문1
원문
A
B
키1로 복호화
A
B
키2로 복호화

【도 4】


시작
S101
인증
S102
원문의 일부영역에서
제2 암호화키 추출
S103
제1 암호화키로 원문중
일부영역 암호화
S104
제2 암호화키로 나머지 영역 암호화
및 암호문 전송
S105
제1 암호화키를 안전한
전송통로로 전송
S106
영역분할 정보와
제2 암호화키 정보(크기, 위치)를
안전한 전송통로로 전송
S107
수신된 제1암호화키로 암호문
일부영역 복호화
S108
복호화된 일부영역에서
제2 암호화키 추출
S109
제2 암호화키로 나머지 영역
복호화
끝